Annex Auftragsverarbeitung

Im Rahmen der Nutzung des von der Telefónica Germany GmbH & Co. OHG bereitgestellten Dienst Digital Phone werden regelmäßig personenbezogene Daten verarbeitet. Sie sind gemäß gesetzlicher Regelungen dazu verpflichtet, mit der Telefónica Germany GmbH & Co. OHG (nachfolgend Auftragnehmer) einen Vertrag über die Auftragsverarbeitung abzuschließen.

Vertragspartner sind die Telefónica Germany GmbH & Co. OHG, Georg-Brauchle-Ring 50, 80992 München, und der Kunde.

Dieser Annex konkretisiert die datenschutzrechtlichen Verpflichtungen der Vertragspartner, die sich aus der Beauftragung des Auftragnehmers („**Hauptvertrag**“) ergeben. Der Annex findet Anwendung auf alle Tätigkeiten, bei denen der Auftragnehmer personenbezogene Daten oder Daten, die dem Fernmeldegeheimnis unterliegen („**Auftraggeber-Daten**“), verarbeitet. Für diesen Annex gelten die Begriffsbestimmungen der EU-Datenschutzgrundverordnung („DS-GVO“) sowie des Bundesdatenschutzgesetzes 2017 („BDSG 2017“), sofern nichts Abweichendes bestimmt wurde.

§ 1 Vertragsgegenstand, Zweck der Datenverarbeitung, Verantwortlichkeit

(1) Zweck, Art und Umfang der Verarbeitung von Auftraggeber-Daten im Sinne dieses Vertrags sowie die Art der Daten und der Kreis der betroffenen Personen ergeben sich aus den **Anlagen 1 und 2**.
(2) Der Auftraggeber bleibt im Rahmen dieses Vertrages Verantwortlicher im Sinne des Art. 4 Nr. 7 DS-GVO. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich.
(3) Die Inhalte dieses Vertrags gelten auch für Tätigkeiten des Auftragnehmers im Auftrag des Auftraggebers, bei denen ein Zugriff auf Auftraggeber-Daten durch den Auftragnehmer nicht ausgeschlossen werden kann (bspw. Prüfung oder Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen im Auftrag).

§ 2 Dauer des Auftrags

(1) Die Laufzeit dieses Vertrages entspricht – sofern ein Hauptvertrag geschlossen wurde – der im Hauptvertrag vereinbarten Laufzeit. Dieser Vertrag endet mit dem Hauptvertrag, ohne dass es einer separaten Kündigung dieses Vertrages bedarf. Die Parteien können diesen Vertrag nur mit dem zugrunde liegende Hauptvertrag kündigen; sofern im Hauptvertrag nichts Abweichendes vereinbart wurde.
(2) Sofern kein Hauptvertrag geschlossen wurde wird dieser Vertrag auf unbestimmte Zeit geschlossen. Die Kündigungsfrist beträgt in diesem Fall drei (3) Monate.

§ 3 Weisungsgebundene Verarbeitung und Mitteilungspflicht bei vermuteten Verstößen

(1) Der Auftragnehmer darf Auftraggeber-Daten nur auf dokumentierte Weisung des Auftraggebers – auch in Bezug auf die Übermittlung von Auftraggeber-Daten an ein Drittland oder eine internationale Organisation – verarbeiten, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, hierzu verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.
(2) Weisungen werden vom Auftraggeber grundsätzlich in Textform (z.B. per E-Mail) erteilt. Soweit eine Weisung ausnahmsweise mündlich erfolgt, wird diese vom Auftraggeber entsprechend in Textform (z.B. per E-Mail) bestätigt.
(3) Der Auftragnehmer wird den Auftraggeber unverzüglich darauf hinweisen, wenn die Befolgung einer vom Auftraggeber erteilten Weisung nach seiner Ansicht gegen die DS-GVO oder eine andere Vorschrift über den Datenschutz verstößt.

§ 4 Vertraulichkeits-/ Verschwiegenheitspflicht

Der Auftragnehmer wird zur Durchführung des Vertrages nur Personen beschäftigen, die er zur Vertraulichkeit verpflichtet hat oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 5 Sicherheit der Verarbeitung / Technische und organisatorische Maßnahmen gemäß Art. 32 DS-GVO

(1) Der Auftragnehmer ergreift alle erforderlichen technischen und organisatorischen Maßnahmen gem. Artikel 32 DS-GVO. Diese werden in **Anlage 3** spezifiziert.
(2) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Während der Dauer dieses Auftrags sind diese durch den Auftragnehmer fortlaufend an die Anforderungen dieses Auftrags anzupassen und dem technischen Fortschritt entsprechend weiterzuentwickeln. Das Sicherheitsniveau der hier und in **Anlage 3** festgelegten technischen und organisatorischen Maßnahmen darf nicht unterschritten werden.
(3) Der Auftragnehmer verpflichtet sich, Änderungen der technischen und organisatorischen Maßnahmen, die einen wesentlichen Einfluss auf das gewährleistete Sicherheitsniveau haben, als Ergänzung der **Anlage 3** schriftlich zu dokumentieren, was auch in einem elektronischen Format erfolgen kann, und dem Auftraggeber zur Kenntnis zu geben.

§ 6 Inanspruchnahme der Dienste weiterer Auftragsverarbeiter

(1) Der Auftragnehmer darf weitere Auftragsverarbeiter (im Folgenden: „Subunternehmer“) in Anspruch nehmen. Die zum Zeitpunkt des Vertragsschlusses in Anspruch genommenen Subunternehmer sind in **Anlage 4** zu diesem Vertrag aufgeführt. Der Auftragnehmer hat den Auftraggeber schriftlich, was auch in einem elektronischen Format erfolgen kann, über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von Subunternehmern zu informieren. Gegen derartige Änderungen kann der Auftraggeber nach erfolgter Information durch den Auftragnehmer binnen 14 Tagen Einspruch erheben.
(2) Nimmt der Auftragnehmer die Dienste eines Subunternehmers in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, so werden diesem Subunternehmer im Wege eines Vertrags, der schriftlich abzufassen ist, was auch in einem elektronischen Format erfolgen kann, oder eines anderen Rechtsinstruments nach dem Unionsrecht oder dem Recht des betreffenden Mitgliedstaats dieselben Datenschutzpflichten auferlegt, die in diesem Vertrag festgelegt sind, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DS-GVO erfolgt. Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten jenes Subunternehmers.

§ 7 Mitwirkungs-/ Unterstützungspflichten

Der Auftragnehmer unterstützt den Auftraggeber angesichts der Art der Verarbeitung mit geeigneten technischen organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Person nachzukommen (Berücksichtigung von Betroffenenrechten hinsichtlich der Gewährleistung von Transparenz; Recht auf Auskunft; Berichtigungsrecht; Recht auf Löschung („Vergessenwerden“); Recht auf Einschränkung der Verarbeitung; Mitteilungsrecht bei Berichtigung und Löschung sowie Einschränkung der Verarbeitung; Recht auf Datenübertragbarkeit; Widerspruchsrecht; Rechte bei automatisierten Einzelfallentscheidungen).

§ 8 Haftung

Die Haftungs- und Schadensersatzvereinbarungen aus dem Hauptvertrag, soweit sie getroffen wurden finden auf diesen Annex Anwendung.

§ 9 Unterstützung bei der Erfüllung von Auftraggeberpflichten

Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DS-GVO genannten Pflichten (Gewährleistung der Sicherheit der Verarbeitung; Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörden; Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person; Datenschutz-Folgenabschätzung; Vorherige Konsultation).

§ 10 Löschung und Rückgabe von Auftraggeber-Daten

Soweit gesetzliche oder anderweitige Aufbewahrungspflichten nicht entgegenstehen, wird der Auftragnehmer nach Beendigung des Auftrags auf Weisung des Auftraggebers die Auftraggeber-Daten dem Auftraggeber in einer für den Auftraggeber lesbaren und bearbeitbaren Form herausgeben oder die Auftraggeber-Daten löschen.

§ 11 Pflichtennachweis und Unterstützung bei Überprüfungen

Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DS-GVO niedergelegten Pflichten zur Verfügung. Er ermöglicht Überprüfungen – einschließlich Inspektionen –, die vom Auftraggeber oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu ihrer Durchführung bei. Der Auftragnehmer kann die Einhaltung seiner Pflichten aus Art. 28 DS-GVO, insbesondere die Umsetzung der ergriffenen technischen und organisatorischen Maßnahmen auch durch Vorlage von Zertifikaten (IT-Sicherheits- oder Datenschutzaudits z.B. nach BSI-Grundschutz), Prüfberichten von unabhängigen Instanzen (z.B. Datenschutzbeauftragter, Datenschutz-/ Qualitätsauditoren, Wirtschaftsprüfer, Revision, IT-Abteilung) oder Auszügen hieraus nachweisen.

§ 12 Sonstiges, Allgemeines

(1) Die folgenden **Anlagen** sind wesentlicher Bestandteil dieses Vertrages:

- **Anlage 1:** Allgemeine Angaben zum Auftrag sowie zu Gegenstand, Art und Umfang der Datenverarbeitung.
- **Anlage 2:** Festlegung der Zwecke der Verarbeitung der Auftraggeber-Daten sowie der Art der Daten und des Kreises der betroffenen Personen
- **Anlage 3**: Beschreibung der technischen und organisatorischen Maßnahmen, die der Auftragsverarbeiter gemäß § 5 dieses Vertrages eingeführt hat
- **Anlage 4**: Angaben zu Subunternehmern des Auftragnehmers.

(2) Die Regelungen dieses Vertrags gehen abweichenden Regelungen in einem ggf. geschlossenen Hauptvertrag vor, soweit dieser Vertrag nicht ausdrücklich anderes bestimmt.
(3) Sollte eine Bestimmung dieses Vertrages unwirksam sein oder werden, oder eine an sich notwendige Regelung nicht enthalten sein, so wird dadurch die Wirksamkeit der übrigen Bestimmungen dieses Vertrages nicht berührt. Anstelle der unwirksamen Bestimmung oder zur Ausfüllung der Regelungslücke gilt eine rechtlich zulässige Regelung, die so weit wie möglich dem entspricht, was die Parteien gewollt haben oder nach Sinn und Zweck dieses Vertrages gewollt hätten, wenn sie die Regelungslücke erkannt hätten.

Anlage 1: Allgemeine Angaben zum Auftrag sowie zu Gegenstand, Art und Umfang der Datenverarbeitung

1.1	Beschreibung der konkreten Datenverarbeitung (Gegenstand, Art und Umfang)	Telefónica Germany stellt dem Kunden den Service „Digital Phone“ zur Verfügung. Dies umfasst die Bereitstellung von VoIP-basierten Telekommunikationsdienstleistungen wie z.B. Sprachverbindungen, virtuelle Konferenzen, Anrufweiterleitungen oder Warteschleifen. Die Funktionen werden über eine zentrale, cloud-gehostete Telefonanlage zur Verfügung gestellt. Die Infrastruktur dieser sogenannten virtuellen Telefonanlage wird in georedundanten Rechenzentren in Deutschland betrieben. Auf die Funktionen und Konfigurationsmöglichkeiten dieser virtuellen Telefonanlage kann der Kunde webbasiert zugreifen. Bei der Bereitstellung von Digital Phone werden die Stammdaten des Kunden verarbeitet. Die Stammdaten werden hierbei im Customer-Relationship-Management-System (CRM) von Telefónica Germany sowie in der virtuellen Telefonanlage selbst hinterlegt. Des Weiteren werden folgende Tätigkeiten durch Telefónica Germany durchgeführt: - Aufsetzen und konfigurieren der virtuellen Telefonanlage inkl. Bestands-/ und Standortdaten und hinterlegen der gebuchten Produkte. - Bestellung und Einrichtung von Rufnummern - Bereitstellung von elektronischen Abrechnungsdaten (Einzelverbindungsnachweis) - 2nd Level Support, Verkehrsdatenanalyse, Überprüfung von Konfigurationsfehlern, Analyse von Callflows - Unterstützung des Kunden bei Netzwerkkonfigurationen.
1.2	E-Mail-Adresse zur Meldung von Datenschutzvorfällen (§ 2 Abs. 7)	Email: datenschutz@telefonica.com
1.3	Betriebsstätte des Auftragnehmers	Anschrift: Telefónica Germany GmbH & Co. OHG Georg-Brauchle-Ring 50 80992 München
1.4	Weisungsbefugte Personen/ Abteilungen gegenüber dem Auftragnehmer	Bevollmächtigte oder Weisungsbefugte Personen auf Seiten des Kunden die dem Auftragnehmer im Rahmen der Auftragserteilung oder während der Vertragslaufzeit mitgeteilt wurden.
	Weisungsempfänger auf Seiten des Auftragnehmers	Fachbereich: Business Digital Team E-Mail-Adresse: Business-digital-team@o2.com
1.5	Hauptvertrag (Purchase Order-/ Vertragsbezeichnung):	Auftragsformular inkl. weitere Vertragsanlagen sowie ggfls. individueller Rahmenvertrag
1.6	Beginn der Verarbeitung	Nach Unterzeichnung des Auftragsformulars durch den Kunden
1.7	Geplante Dauer des Auftrags	Maßgeblich ist die gewählte Vertragslaufzeit sowie die einschlägigen Kündigungsfristen

Anlage 2: Festlegung von Zweck der Verarbeitung der Auftraggeber-Daten sowie der Art der Daten und des Kreises der betroffenen Personen

2.1	**Zweck der** Tätigkeit des Auftragnehmers	**Zwecke bezüglich Teilnehmer (Kunde eines TK-Dienstes)/ Nutzer (Nutzer des TK-Dienstes, der selbst nicht Kunde ist)** ☒ Gestaltung und/ oder Erbringung eines Telekommunikationsdienstes (z.B. Netzbetrieb) ☒ Ermittlung des Entgelts und Abrechnung mit den Teilnehmern (z.B. Rechnungs-/ EVN-Erstellung) ☒ Verwendung für die Bereitstellung von Diensten mit Zusatznutzen (z.B. location based services) ☒ Verwaltung von Teilnehmerdaten (z.B. Betrieb eines CRM-Systems) ☒ Analyse/ Auswertung für Zwecke der bedarfsgerechten Gestaltung von Telekommunikations- und/ oder Telemediendiensten (z.B. BI, Netzwerkausbau) ☒ Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen
2.2	**Datenkate-gorien** die durch den Auftragnehmer verarbeitet werden	**1. Daten bezüglich Teilnehmer (Kunde eines TK-Dienstes) / Nutzer (Nutzer des TK-Dienstes, der selbst nicht Kunde ist)** ☒ Bestandsdaten nach dem TKG (Vertragliche Angaben, wie Name, Adresse, Bankverbindung, Geburtsdatum, MSIDSN, IMEI, IMSI, Kundennummer, Rechnungsnummer, E-Mail-Adresse etc.) ☒ Kundenumsätze/ Revenue ☒ Rechnungen ☒ Bank- oder Kreditkartendaten ☒ Legitimationspapiere (Personalausweiskopie, Personalausweisnummer, Reisepass etc.) ☒ Bonitätsinformationen ☒ Kundenhistorie ☒ Kundenkommunikation ☒ Informationen zu genutzter Hardware oder installierter Software (z.B. Geräte-ID, IMEI, TAC) ☒ Verkehrsdaten (Daten, die einen konkreten Telekommunikationsvorgang betreffen, wie A-Rufnummer, B-Rufnummer, Uhrzeit, Dauer, genutzter Dienst, Call Data Records, Einzelverbindungsnachweis, IP-Adresse) ☒ Standortdaten (Daten zur Identifizierung eines Standorts eines Endgeräts, Cell-ID, GPS-Daten) ☒ Inhaltsdaten (Inhalte der Kommunikation, z.B. E-Mail-Inhalte, Gesprächsinhalte, Datenstrom ab OSI-Layer 4, etc.) ☒ Bestandsdaten nach dem Telemediengesetz (z.B. Name, Anschrift des Nutzers von Websites und Apps, etc.) ☒ Nutzungsdaten nach dem Telemediengesetz (Beginn, Ende, Umfang der jeweiligen Nutzung z.B. von Websites oder Apps, IP-Adresse etc.) **2. Daten bezüglich Mitarbeitern** ☒ Berufliche Kontaktdaten von Mitarbeitern, Zeitarbeitern, Praktikanten, Auszubildenden (berufliche Telefonnummer/ E-Mailadresse, Abteilungszugehörigkeit)
2.3	Folgende Daten von **betroffenen Personen** werden durch den Auftrag-nehmer verarbeitet	☒ TK-Dienste-Teilnehmer (Kunde eines TK-Dienstes) ☒ TK-Dienste-Nutzer (Nutzer des TK-Dienstes, der selbst nicht Kunde ist)

2.4	Folgende Vorgaben für die **Datenlöschung** werden berücksichtigt	Die Auftraggeber-Daten (insbesondere Bestands-/ Verkehrs-/ Inhalts- und Mitarbeiterdaten) werden gelöscht, wenn sie für die Durchführung des Auftrags nicht mehr erforderlich sind, es sei denn es liegt eine abweichende Weisung des Auftraggebers vor. Die Löschung von Verkehrsdaten erfolgt entsprechend den rechtlichen Anforderungen aus dem “Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten”.

Anlage 3: Beschreibung der technischen und organisatorischen Maßnahmen, die der Auftragsverarbeiter gemäß § 2 Abs. 9 dieses Vertrages eingeführt hat

3.1	**Ergebnis der Schutzbedarfsanalyse** Der Auftragnehmer hat den Schutzbedarf der Daten wie folgt definiert:				
	Definition	**Vertraulichkeit** *Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden. Dies gilt sowohl beim Zugriff auf gespeicherte Daten wie auch während der Datenübertragung.*	**Integrität** *Daten dürfen nicht unbemerkt oder unautorisiert verändert werden. Alle etwaigen Änderungen müssen nachvollziehbar sein (Daten- & Systemintegrität).*	**Verfügbarkeit** *Der Zugriff auf die Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet werden; Verhinderung von Systemausfällen.*	**Belastbarkeit** *Toleranz und Ausgleichsfähigkeit eines Systems gegen Störungen/ Angriffe von innen und außen (Widerstandsfähigkeit, Ausfallsicherheit).*
	Sehr hoch	☒	☐	☐	☐
	Hoch	☐	☒	☒	☒
	Mittel	☐	☐	☐	☐
	Niedrig	☐	☐	☐	☐
	Sehr niedrig	☐	☐	☐	☐
	Nicht relevant	☐	☐	☐	☐

3.2	Ein **Sicherheitskonzept** gemäß Art. 32 DS-GVO liegt vor	
3.3	Gemäß der technisch organisatorischen Maßnahmen (toM) sind Maßnahmen zur **Pseudonymisierung von** personenbezogenen Daten ergriffen worden.	
3.4	Folgende Maßnahmen sind zur räumlichen **Zutrittskontrolle** ergriffen worden, die es Unbefugten verwehren, sich den Systemen, Datenverarbeitungsanlagen oder Verfahren physisch zu nähern, mit denen personenbezogene Daten verarbeitet werden.	☒Schlüsselverwaltung/ Dokumentation der Schlüsselvergabe ☒ Zutrittskontrollsystem, z.B. Ausweisleser (Magnet-/Chipkarten) ☒ Sicherheitstüren / -fenster ☒ Türsicherungen (elektrische Türöffner, Zahlenschloss, etc.) ☒ Alarmanlage ☒ Videoüberwachung ☒ Spezielle Schutzvorkehrungen des Serverraums
3.5	Folgende Maßnahmen zur **Zugangskontrolle** wurden ergriffen, die gewährleisten, dass ein Zugang durch Unbefugte auf Datenverarbeitungssysteme verhindert wird.	☒ Benutzer haben einen eindeutigen persönlichen Bezeichner ☒ Benutzerkennungen werden, wenn die Benutzer das Unternehmen verlassen haben, gelöscht oder deaktiviert ☒ Passwörter werden grundsätzlich nicht im Klartext gespeichert oder unverschlüsselt übertragen ☒ Sichere Passwortverfahren ☒ Zwei-Faktor-Authentifizierung für kritische Anwendungen ☒ Automatische Sperrung der Clients nach Zeitablauf ohne Useraktivität (bspw. passwortgeschützter Bildschirmschoner) ☒ Regelmäßige Softwareaktualisierung / Patching (Patchmanagement) ☒ Firewall, IDS/IPS

3.6	Folgende Maßnahmen zur **Zugriffskontrolle** wurden ergriffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.	☒ Kryptokonzept vorhanden ☒ Inventarisierung der Informationstechnik ☒ Verwaltung und Dokumentation von Berechtigungen ☒ Differenzierte Berechtigungen ☒ Aufgabenbezogene Profile ☒ Aufgabenbezogene Rollen ☒ Genehmigungsroutinen ☒ Regelmäßige Prüfung der Aktualität von Zugriffsrechten ☒ Auswertungen/ Protokollierungen ☒ Prüfung/Auditierung (z.B. ISO-Zertifizierung, SOX-Compliance) ☒ Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops (z.B. Betriebssystem, True Crypt, Safe Guard Easy, WinZip, PGP) ☒ Vier-Augen-Prinzip ☒ Passwort-Identifikation, etc.
3.7	Folgende Maßnahmen zur **Weitergabekontrolle** wurden ergriffen, die gewährleisten dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.	☒ Verschlüsselung von E-Mail (Ende-zu-Ende) ☒ Getunnelte Datenfernverbindungen (VPN = Virtual Private Network) ☒ Gesichertes WLAN ☒ SSL-/TLS-Verschlüsselung ☒ Verschlüsselung von CD/DVD-ROM, externen Festplatten und/oder Laptops ☒ Regelungen zur Datenträgervernichtung, etc. ☒ Sichere, rückstandsfreie Löschung ☒ Sonstiges*:* ☒ Protokollierung der Datenweitergabe
3.8	Folgende Maßnahmen zur **Eingabekontrolle** wurden ergriffen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungs-systeme eingegeben, verändert oder entfernt worden sind.	☒ Inventarisierung der für den Auftrag relevanten Daten ☒ Berechtigungskonzepte vorhanden, inkl.: ☒ Funktionale Verantwortlichkeiten ☒ Zugriffsrechte ☒ Systemseitige Protokollierungen ☒ Funktionelle Verantwortlichkeiten ☒ Mehraugenprinzip
3.9	Folgende Maßnahmen zur **Auftragskontrolle** wurden ergriffen, die sicherstellen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.	☒ Verbindliche Sicherheitsleitlinien inkl. Verpflichtungen der Mitarbeiter ☒ Schulungen aller zugriffsberechtigten Mitarbeiter ☒ Regelmäßig stattfindende Nachschulungen ☒ Regelmäßige Datenschutzaudits des betrieblichen Datenschutzbeauftragten ☒ Prüfungsplanung für interne und externe Audits ☒ Monitoring & Reporting über neu Identifizierte Risiken / Schwachstellen ☒ IT Change Management Prozess

		☒ Trennung von Entwicklungs- und Produktivsystemen inkl. geregeltem Transportprozess (production take over) ☒ Genehmigungs- und Freigabeverfahren ☒ Regeln für die sichere Entwicklung von Software und Systemen sind festgelegt und werden angewandt
3.10	Folgende Maßnahmen zur **Verfügbarkeitskontrolle** wurden ergriffen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind bzw. zügig wiederhergestellt werden können.	☒ Service Level Agreements (SLAs) mit Dienstleistern ☒ Backup Verfahren ☒ Viren-/Schadcodeschutz ☒ sichere Aufbewahrung für Backups (z.B. Safe, getrennter Brandabschnitt) ☒ Redundanz (z.B. Spiegeln von Festplatten) ☒ redundante Versorgung (z.B. Internet, Telefon, Strom) ☒ Firewall, IDS/IPS ☒ Brandschutz und Löschwasserschutz ☒ Monitoring von Alarmen ☒ Pläne für Ausfall/ Notfall/ Wiederherstellung, etc..
3.11	Folgende Maßnahmen zur Einhaltung des **Trennungsgebots** wurden ergriffen, die gewährleisten, dass Daten, die zu unterschiedlichen Zwecken erhoben werden, getrennt verarbeitet (z.B. gelöscht) werden können.	☒ Rechte- und Rollenkonzepte ☒ Trennung durch Zugriffsregelungen ☒ Sonstiges: logische Mandantentrennung
3.12	Folgende Maßnahmen und Verantwortlichkeiten für den **Umgang mit Informations-sicherheitsvorfällen und Krisensituationen** wurden definiert.	☒ Managementprozess für Security Incidents ☒ Managementprozess für datenschutzrelevante Incidents ☒ Definition der Sicherheitsanforderungen in Krisensituation / im Notfall ☒ Übergreifender Notfallplan inkl. regelmäßiger Aktualisierung ☒ Business Continuity Management
3.13	Folgende Maßnahmen für **Logging** in den relevanten Bereichen wurden ergriffen.	☒ Die Log-Systeme beziehen sich auf eine einzige Zeitquelle ☒ Verarbeitung der Daten in Übereinstimmung mit geltenden gesetzlichen Bestimmungen für die Informationssicherheit ☒ Logs sind gegen unberechtigten Zugriff geschützt (Vertraulichkeit) ☒ Logs sind vor unberechtigter Veränderung geschützt (Integrität) ☒ Logs sind vor Verlust geschützt (Verfügbarkeit) Maßnahmen zur Eingabekontrolle: - Festlegung, was protokolliert wird, insbesondere die Eingabe, Änderung und Löschung von Daten werden protokolliert und sechs Monate gespeichert. - Sichere Aufbewahrung von Protokollinformationen - Ein mehrstufiges Berechtigungskonzept sorgt dafür, dass unterschiedliche Benutzer unterschiedliche Rechte zur Eingabe, Änderung und Löschung von Daten in der Portaloberfläche haben. - Der Zugriff auf die Portaloberflächen erfolgt mittels individueller Benutzernamen und Passwörter.
3.14	Folgende Maßnahmen zur Arbeit im Homeoffice bzw. für Telearbeit wurden ergriffen.	☒ Homeoffice Richtlinie / Richtlinie mobiles Arbeiten ☒ Untersagung mobiles Arbeiten in öffentlichen Bereichen ☒ Endgerät ist nach dem Stand der Technik geschützt ☒ Regelmäßige Bestätigung der Einhaltung der Homeofffice Richtlinie

		☒ Verschlüsselung der Remoteverbindung ☒ Zwei-Faktor-Authentifizierung ☒ Organisatorische und physische Maßnahmen zur Gewährleistung der Vertraulichkeit ☒ Schutz vor Datenweitergabe vom Endgerät

Anlage 4: Angaben zu Subunternehmern des Auftragnehmers

Zur Erfüllung des Vertrages/Hauptvertrages werden bzw. wurden Subunternehmer mit der Erbringung eines Teils der Dienstleistung beauftragt:

Angabe des Subunternehmers/ Konzernunternehmen	**Ort der Speicherung/ des bestimmungsgemäßen Zugriffs auf Auftraggeber-Daten** [*falls abweichend von Anschrift des Subunternehmers]*	**Erfolgt eine Datenverarbeitung oder ein Zugang zu Auftraggeber-Daten aus Drittstaaten (außerhalb der EU/ EWR)?** *[z.B. durch Beauftragung von weiteren Dienstleistern durch den beauftragten Subunternehmer]*	**Gegenstand der Unterbeauftragung und verarbeitete Kategorien von Auftraggeber-Daten**	**Abgeschlossener ADV-Vertrag / EU-Standardvertrag** **Der zwischen Auftragnehmer und Subunternehmer abgeschlossene ADV-Vertrag nach Art. 28 DS-GVO/ EU Model Clauses ist vor dem Abschluss dieses Vertrags auf Anforderung vorzulegen.**
Name/ Firma: NFON AG Anschrift: Machtlfinger Str. 7, 81379 München Kontaktdaten der Datenschutzabteilung: datenschutz@nfon.com	Anschrift: Rechenzentrum München Rechenzentrum Nürnberg	☐Ja, *[bitte spezifizieren, welcher Dienstleister, Anschrift/ Ort des möglichen Datenzugangs, Art der Tätigkeit und Datenarten]* ☒Nein, ein Zugang zu Auftraggeber-Daten ist ausgeschlossen	Bereitstellung der virtuellen Telefonanlage für den Dienst Digital Phone	☒Ja, liegt vor ☐Nein, weil